PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-374308
(43)Date of publication of application : 26.12.2002

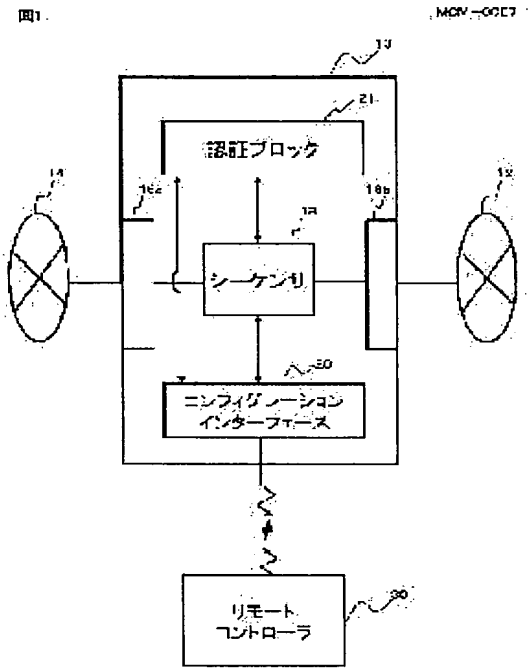
(51)Int.CI. H04L 12/66
G06F 13/00
G09C 1/00
H04L 9/14

(21)Application number : 2001-178427
(22)Date of filing : 13.06.2001

(71)Applicant : MCM JAPAN KK
(72)Inventor : SANETO TORU

(54) COMMUNICATIONS EQUIPMENT FOR TRANSMISSION AND CONTROLLING DEVICE FOR THE SAME

(57)Abstract:
PROBLEM TO BE SOLVED: To realize safety communication, without using authentication servers.
SOLUTION: A configuration interface 20 automatically generates a cryptographic key, based on data communication between with an external remote controller 30. Then, the generated cryptographic key is transmitted to the controller 30 and sent to an authentication block 21. A sequencer 18 deciphers a packet sent from an external network 12, by using the cryptographic key. The sequencer 18 ciphers the packet sent from an internal network 14 by using the cryptographic key. The controller 30, receiving the cryptographic key, stores the cryptographic key in a memory means 36. The cryptographic key inside of the memory means 36 is introduced to another fire wall module via the controller 30. The same cryptographic key can be set easily among a plurality of fire wall modules, to realize cipher communication.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's

decision of rejection]
[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－374308
（P2002－374308A）
(43)公開日　平成14年12月26日(2002.12.26)

(51)Int.Cl.⁷	識別記号	ＦＩ		テーマコード（参考）
Ｈ０４Ｌ　12/66		Ｈ０４Ｌ　12/66	Ｂ	５Ｂ０８９
Ｇ０６Ｆ　13/00	３５１	Ｃ０６Ｆ　13/00	３５１Ｚ	５Ｊ１０４
Ｇ０９Ｃ　1/00	６６０	Ｇ０９Ｃ　1/00	６６０Ｅ	５Ｋ０３０
Ｈ０４Ｌ　9/14		Ｈ０４Ｌ　9/00	６４１	

審査請求　未請求　請求項の数19　ＯＬ　（全 15 頁）

(21)出願番号　特願2001－178427(P2001－178427)

(22)出願日　平成13年６月13日(2001.6.13)

(71)出願人　595161887
エム・シー・エムジャパン株式会社
東京都世田谷区三軒茶屋２－11－22　サンタワーズセンタービル

(72)発明者　実藤　亨
東京都世田谷区三軒茶屋２丁目11番22号　サンタワーズセンタービル　エム・シー・エムジャパン株式会社内

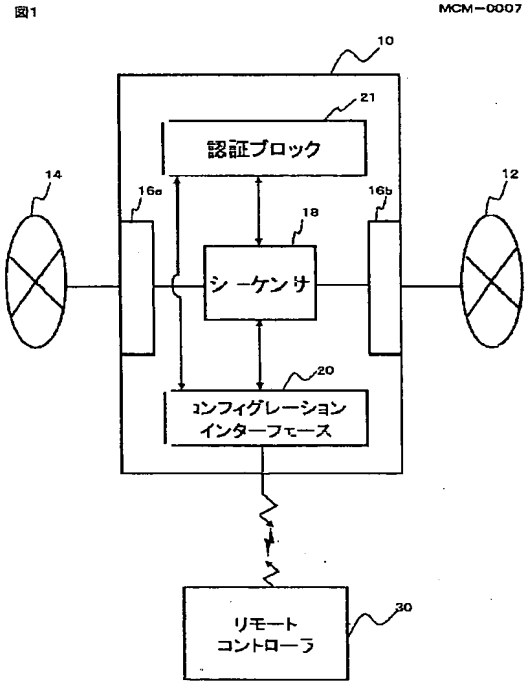
(74)代理人　100109014
弁理士　伊藤　充

最終頁に続く

(54)【発明の名称】　伝送用通信機器及びこれを制御する制御機器

(57)【要約】
【課題】認証サーバを用いずに安全な通信を実現する。
【解決手段】コンフィグレーションインターフェース２０は、外部のリモートコントローラ３０とのデータ通信に基づき、暗号鍵を自動生成する。そして、生成した暗号鍵は、リモートコントローラ３０に送信されると共に、認証ブロック２１に送られる。シーケンサ１８は、この暗号鍵を用いて外部ネットワーク１２から送られてきたパケットを復号化する。シーケンサ１８は、この暗号鍵を用いて内部ネットワーク１４から送られてきたパケットを暗号化する。暗号鍵を受け取ったリモートコントローラ３０はその暗号鍵をメモリ手段３６に格納する。そのメモリ手段３６内部の暗号鍵をリモートコントローラ３０を介して他のファイアーウォールモジュール１０に導入させる。複数のファイアーウォールモジュール１０間で容易に同一の暗号鍵を設定することができ、暗号通信を実現できる。

図1



【特許請求の範囲】
【請求項１】　外部ネットワークと、内部ネットワークとを結ぶ伝送用通信機器において、
前記内部ネットワークから送信されたパケットを暗号化してから前記外部ネットワークに送り出し、前記外部ネットワークから送信されてきたパケットを復号化してから前記内部ネットワークに送り出す暗号化復号化手段を含み、
前記暗号化復号化手段は、
パケット情報と、そのパケット情報に対応した暗号化ビットと、を含むアクセステーブルを備え、
前記暗号化復号化手段は、前記内部ネットワークから送信された前記パケットのパケット情報を前記アクセステーブルから検索し、前記パケット情報に対応した前記暗号化ビットの値を読み出し、前記暗号化ビットが立っている場合に、前記パケットを暗号化することを特徴とする伝送用通信機器。
【請求項２】　請求項１記載の伝送用通信機器において、
前記暗号化復号化手段は、前記外部ネットワークから送信された前記パケットのパケット情報を前記アクセステーブルから検索し、前記パケット情報に対応した前記暗号化ビットの値を読み出し、前記暗号化ビットが立っている場合に、前記パケットを復号化することを特徴とする伝送用通信機器。
【請求項３】　請求項１又は２記載の伝送用通信機器において、
前記パケット情報は、ＩＰフィールドの情報、又は、ＴＣＰ／ＵＤＰフィールドの情報を含むことを特徴とする伝送用通信機器。
【請求項４】　請求項１又は２記載の伝送用通信機器において、
前記暗号鍵を生成する暗号鍵管理手段、
を含み、前記暗号鍵管理手段は、外部から暗号鍵生成の指示がなされた場合に、前記暗号鍵を生成し、生成した暗号鍵を外部に送信することを特徴とする伝送用通信機器。
【請求項５】　請求項４記載の伝送用通信機器において、
前記暗号鍵管理手段は、外部と無線による通信を行い、前記外部からの指示は、前記無線による通信によって受信することを特徴とする伝送用通信機器。
【請求項６】　請求項４記載の伝送用通信機器において、
前記暗号鍵管理手段は、外部と赤外線による通信を行い、前記外部からの指示は、前記赤外線による通信によって受信することを特徴とする伝送用通信機器。
【請求項７】　請求項１又は２記載の伝送用通信機器において、
前記暗号鍵を生成する暗号鍵管理手段と、
着脱可能な可搬型のメモリ手段にデータを書き込むメモリインターフェースと、
を含み、前記暗号鍵管理手段は、外部から暗号鍵生成の指示がなされた場合に、前記暗号鍵を生成し、生成した暗号鍵を前記メモリインターフェースを介して前記メモリ手段に格納することを特徴とする伝送用通信機器。
【請求項８】　伝送用通信機器に対して、指示を出す制御機器において、
前記伝送用通信機器と無線による通信を行う通信手段と、
利用者の操作に基づき、暗号鍵の生成の指示を前記通信手段を介して前記伝送用通信機器に対して行う制御手段と、
を含み、
前記制御手段は、前記通信手段を介して前記伝送用通信機器から前記生成を指示した暗号鍵が送信されてきた場合に、その暗号鍵を着脱可能な可搬型のメモリ手段に格納することを特徴とする制御機器。
【請求項９】　伝送用通信機器に対して、指示を出す制御機器において、
前記伝送用通信機器と赤外線による通信を行う通信手段と、
利用者の操作に基づき、暗号鍵の生成の指示を前記通信手段を介して前記伝送用通信機器に対して行う制御手段と、
を含み、
前記制御手段は、前記通信手段を介して前記伝送用通信機器から前記生成を指示した暗号鍵が送信されてきた場合に、その暗号鍵を着脱可能な可搬型のメモリ手段に格納することを特徴とする制御機器。
【請求項１０】　請求項４記載の伝送用通信機器において、
前記暗号鍵を格納する暗号鍵格納手段、
を有し、
前記暗号鍵管理手段は、前記外部から前記暗号鍵が送信されてきた場合に、前記送信されてきた暗号鍵を前記暗号鍵格納手段に格納することを特徴とする伝送用通信機器。
【請求項１１】　請求項７記載の伝送用通信機器において、
前記暗号鍵を格納する暗号鍵格納手段、
を有し、
前記暗号鍵管理手段は、前記メモリインターフェースを介して、前記メモリ手段に格納されている暗号鍵を読み出し、読み出した前記暗号鍵を前記暗号鍵格納手段に格納することを特徴とする伝送用通信機器。
【請求項１２】　請求項８記載の制御機器において、
前記伝送用通信機器と無線による通信を行う通信手段と、
利用者の操作に基づき、前記着脱可能な可搬型のメモリ

手段に格納されている暗号鍵を前記通信手段を介して前記伝送用通信機器に対して送信する制御手段と、
を含むことを特徴とする制御機器。
【請求項１３】　請求項９記載の制御機器において、
前記伝送用通信機器と赤外線による通信を行う通信手段と、
利用者の操作に基づき、前記着脱可能な可搬型のメモリ手段に格納されている暗号鍵を前記通信手段を介して前記伝送用通信機器に対して送信する制御手段と、
を含むことを特徴とする制御機器。
【請求項１４】　コンピュータを伝送用通信機器として動作させるプログラムにおいて、前記コンピュータに、
外部から暗号鍵生成の指示を受信した場合に、この指示に基づき前記暗号鍵を生成する生成手順と、
前記生成した暗号鍵を前記外部に送信する通信手順と、
を実行させることを特徴とするプログラム。
【請求項１５】　請求項１４記載のプログラムにおいて、
前記コンピュータに、
外部から暗号鍵が送信されてきた場合に、前記送信されてきた暗号鍵を、暗号鍵を格納する手段に格納する手順、
を実行させることを特徴とするプログラム。
【請求項１６】　コンピュータを伝送用通信機器として動作させるプログラムにおいて、前記コンピュータに、
外部から暗号鍵生成の指示を受信した場合に、この指示に基づき前記暗号鍵を生成する生成手順と、
前記生成した暗号鍵を、着脱可能なメモリ手段に格納する格納手順と、
を実行させることを特徴とするプログラム。
【請求項１７】　請求項１６記載のプログラムにおいて、
前記コンピュータに、
利用者からの指示に基づき、前記着脱可能なメモリ手段に格納されている暗号鍵を読み出す読み出し手順と、
前記読み出した暗号鍵を、暗号鍵を格納する手段に格納する手順、
を実行させることを特徴とするプログラム。
【請求項１８】　コンピュータを伝送用通信機器として動作させるプログラムを格納した記録媒体において、前記プログラムは、前記コンピュータに、
外部から暗号鍵生成の指示を受信した場合に、この指示に基づき前記暗号鍵を生成する生成手順と、
前記生成した暗号鍵を前記外部に送信する通信手順と、
を実行させることを特徴とするプログラムを格納したコンピュータ読み取り可能な記録媒体。
【請求項１９】　コンピュータを伝送用通信機器として動作させるプログラムを格納した記録媒体において、前記プログラムは、前記コンピュータに、
外部から暗号鍵生成の指示を受信した場合に、この指示に基づき前記暗号鍵を生成する生成手順と、
前記生成した暗号鍵を、着脱可能なメモリ手段に格納する格納手順と、
を実行させることを特徴とするプログラムを格納したコンピュータ読み取り可能な記録媒体。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、伝送用通信機器に関する。特にファイアーウォール（Fire Wall）機能を有する伝送用通信機器に関する。
【０００２】
【従来の技術】近年、ネットワークを介した通信が広く利用されている。また、公衆ネットワークだけでなく、プライベートなネットワークも広く利用されている。このプライベートなネットワークも公衆ネットワークに接続され、外部との間で通信が行えるのが通例である。
【０００３】また、公衆ネットワークを介した通信においては、通信の秘密を守るために、暗号の技術が広く利用されている。この暗号技術の運用の方法は種々知られているが、通信を行う者たち以外の第三者である認証サーバを設ける手法が一般に多く利用されている。
【０００４】
【発明が解決しようとする課題】たとえば、一般の家庭内に設けられているような小規模なプライベートネットワークを利用している者にとってわざわざ認証サーバを利用するのは手続きが煩雑になりがちである。
【０００５】その一方、外部から、自由にこのプライベートなネットワークにアクセスしたいという要求は多い。たとえば、家庭内のプライベートなネットワーク（以下、内部ネットワークと呼ぶ）の利用者が、出張先から家庭の自分のパーソナルコンピュータのハードディスクの内容を見たい場合等が考えられる。この場合、悪意の第三者のアクセスを防止するために、従来は認証サーバを介した煩雑な手続きを踏む必要があった。
【０００６】そのため、認証サーバを使用せずに簡易に安全な通信ができれば便利である。
【０００７】また、内部ネットワークが社内ネットワークである場合でも同様の事情が存在する。たとえば、通常はプライベートな社内ネットワーク上（内部ネットワーク上）で仕事をしつつ、出張の際には外部の出先から社内ネットワーク（内部ネットワーク）にアクセスしたいという要望が現実に考えられる。このような要望を、認証サーバを利用せずに実現できれば円滑に業務を遂行でき便利である。
【０００８】本発明はこのような課題に鑑みなされたものであり、その目的は、認証サーバを利用せずに、安全な通信をネットワーク上で行うことである。
【０００９】
【課題を解決するための手段】本発明は、上記課題を解決するために、外部ネットワークと、内部ネットワーク

とを結ぶ伝送用通信機器において、前記内部ネットワークから送信されたパケットを暗号化してから前記外部ネットワークに送り出し、前記外部ネットワークから送信されてきたパケットを復号化してから前記内部ネットワークに送り出す暗号化復号化手段を含み、前記暗号化復号化手段は、パケット情報と、そのパケット情報に対応した暗号化ビットと、を含むアクセステーブルを備え、前記暗号化復号化手段は、前記内部ネットワークから送信された前記パケットのパケット情報を前記アクセステーブルから検索し、前記パケット情報に対応した前記暗号化ビットの値を読み出し、前記暗号化ビットが立っている場合に、前記パケットを暗号化することを特徴とする伝送用通信機器である。

【0010】このような構成によって、自動的に暗号化を行うことができる伝送用通信機器を実現できる。

【0011】また、本発明は、前記暗号化復号化手段は、前記外部ネットワークから送信された前記パケットのパケット情報を前記アクセステーブルから検索し、前記パケット情報に対応した前記暗号化ビットの値を読み出し、前記暗号化ビットが立っている場合に、前記パケットを復号化することを特徴とする伝送用通信機器である。

【0012】このような構成によって、自動的に暗号化されたパケットを復号化することができる。

【0013】また、本発明は、前記パケット情報は、ＩＰフィールドの情報、又は、ＴＣＰ／ＵＤＰフィールドの情報を含むことを特徴とする伝送用通信機器である。

【0014】このような構成によって、パケットの送信元、宛先を正確に知ることができる。

【0015】また、本発明は、前記暗号鍵を生成する暗号鍵管理手段、を含み、前記暗号鍵管理手段は、外部から暗号鍵生成の指示がなされた場合に、前記暗号鍵を生成し、生成した暗号鍵を外部に送信することを特徴とする伝送用通信機器である。

【0016】このような構成によって、暗号鍵を単に生成させるだけでなく、外部に取り出すことができるので、他の通信機器に暗号鍵を導入することが容易となる。

【0017】また、本発明は、前記暗号鍵管理手段は、外部と無線による通信を行い、前記外部からの指示は、前記無線による通信によって受信することを特徴とする伝送用通信機器である。

【0018】無線による通信を行うので、遠距離から指示を出すことが可能である。

【0019】また、本発明は、前記暗号鍵管理手段は、外部と赤外線による通信を行い、前記外部からの指示は、前記赤外線による通信によって受信することを特徴とする伝送用通信機器である。

【0020】赤外線による通信を行うので、遠距離から指示を出すことが可能である。

【0021】また、本発明は、前記暗号鍵を生成する暗号鍵管理手段と、着脱可能な可搬型のメモリ手段にデータを書き込むメモリインターフェースと、を含み、前記暗号鍵管理手段は、外部から暗号鍵生成の指示がなされた場合に、前記暗号鍵を生成し、生成した暗号鍵を前記メモリインターフェースを介して前記メモリ手段に格納することを特徴とする伝送用通信機器である。

【0022】このような構成によれば、生成した暗号鍵をメモリ手段に自動的に格納することができる。

【0023】また、本発明は、伝送用通信機器に対して、指示を出す制御機器において、前記伝送用通信機器と無線による通信を行う通信手段と、利用者の操作に基づき、暗号鍵の生成の指示を前記通信手段を介して前記伝送用通信機器に対して行う制御手段と、を含み、前記制御手段は、前記通信手段を介して前記伝送用通信機器から前記生成を指示した暗号鍵が送信されてきた場合に、その暗号鍵を着脱可能な可搬型のメモリ手段に格納することを特徴とする制御機器である。

【0024】このような構成によれば、伝送用通信機器に暗号鍵を生成させると共に、その暗号鍵をメモリ手段に格納することができる。

【0025】また、本発明は、伝送用通信機器に対して、指示を出す制御機器において、前記伝送用通信機器と赤外線による通信を行う通信手段と、利用者の操作に基づき、暗号鍵の生成の指示を前記通信手段を介して前記伝送用通信機器に対して行う制御手段と、を含み、前記制御手段は、前記通信手段を介して前記伝送用通信機器から前記生成を指示した暗号鍵が送信されてきた場合に、その暗号鍵を着脱可能な可搬型のメモリ手段に格納することを特徴とする制御機器である。

【0026】このような構成によれば、赤外線通信によって伝送用通信機器に暗号鍵を生成させると共に、その暗号鍵を赤外線通信を用いて受け取ってメモリ手段に格納することができる。

【0027】また、本発明は、前記暗号鍵を格納する暗号鍵格納手段、を有し、前記暗号鍵管理手段は、前記外部から前記暗号鍵が送信されてきた場合に、前記送信されてきた暗号鍵を前記暗号鍵格納手段に格納することを特徴とする伝送用通信機器である。

【0028】このような構成によって、外部からの暗号鍵をその伝送用通信機器に導入させることができる。

【0029】また、本発明は、前記暗号鍵を格納する暗号鍵格納手段、を有し、前記暗号鍵管理手段は、前記メモリインターフェースを介して、前記メモリ手段に格納されている暗号鍵を読み出し、読み出した前記暗号鍵を前記暗号鍵格納手段に格納することを特徴とする伝送用通信機器である。

【0030】このような構成によって、メモリ手段に格納されている暗号鍵をその伝送用通信機器に導入させることができる。

【００３１】また、本発明は、前記伝送用通信機器と無線による通信を行う通信手段と、利用者の操作に基づき、前記着脱可能な可搬型のメモリ手段に格納されている暗号鍵を前記通信手段を介して前記伝送用通信機器に対して送信する制御手段と、を含むことを特徴とする制御機器である。

【００３２】このような構成によって、無線通信を介して暗号鍵を伝送用通信機器に供給することができる。

【００３３】また、本発明は、前記伝送用通信機器と赤外線による通信を行う通信手段と、利用者の操作に基づき、前記着脱可能な可搬型のメモリ手段に格納されている暗号鍵を前記通信手段を介して前記伝送用通信機器に対して送信する制御手段と、を含むことを特徴とする制御機器である。

【００３４】このような構成によって、赤外線通信を介して暗号鍵を伝送用通信機器に供給することができる。

【００３５】また、本発明は、コンピュータを伝送用通信機器として動作させるプログラムにおいて、前記コンピュータに、外部から暗号鍵生成の指示を受信した場合に、この指示に基づき前記暗号鍵を生成する生成手順と、前記生成した暗号鍵を前記外部に送信する通信手順と、を実行させることを特徴とするプログラムである。

【００３６】このようなプログラムを用いれば、暗号鍵を生成する伝送用通信機器を実現することができる。

【００３７】また、本発明は、前記コンピュータに、外部から暗号鍵が送信されてきた場合に、前記送信されてきた暗号鍵を、暗号鍵を格納する手段に格納する手順、を実行させることを特徴とするプログラムである。

【００３８】このようなプログラムを用いれば、送信されてきた暗号鍵を内部に格納する伝送用通信機器を実現することができる。

【００３９】また、本発明は、コンピュータを伝送用通信機器として動作させるプログラムにおいて、前記コンピュータに、外部から暗号鍵生成の指示を受信した場合に、この指示に基づき前記暗号鍵を生成する生成手順と、前記生成した暗号鍵を、着脱可能なメモリ手段に格納する格納手順と、を実行させることを特徴とするプログラムである。

【００４０】このようなプログラムを用いれば、暗号鍵を生成すると共にその暗号鍵をメモリ手段に格納する伝送用通信機器を実現することができる。

【００４１】また、本発明は、前記コンピュータに、利用者からの指示に基づき、前記着脱可能なメモリ手段に格納されている暗号鍵を読み出す読み出し手順と、前記読み出した暗号鍵を、暗号鍵を格納する手段に格納する手順、を実行させることを特徴とするプログラムである。

【００４２】このようなプログラムを用いれば、暗号鍵をメモリ手段から読み取り、内部に格納する伝送用通信機器を実現することができる。

【００４３】また、本発明は、コンピュータを伝送用通信機器として動作させるプログラムを格納した記録媒体において、前記プログラムは、前記コンピュータに、外部から暗号鍵生成の指示を受信した場合に、この指示に基づき前記暗号鍵を生成する生成手順と、前記生成した暗号鍵を前記外部に送信する通信手順と、を実行させることを特徴とするプログラムを格納したコンピュータ読み取り可能な記録媒体である。

【００４４】このような記録媒体をコンピュータに組み込むことによって、暗号鍵を生成する伝送用通信機器を構成することができる。

【００４５】また、本発明は、コンピュータを伝送用通信機器として動作させるプログラムを記録した記録媒体において、前記プログラムは、前記コンピュータに、外部から暗号鍵生成の指示を受信した場合に、この指示に基づき前記暗号鍵を生成する生成手順と、前記生成した暗号鍵を、着脱可能なメモリ手段に格納する格納手順と、を実行させることを特徴とするプログラムを格納したコンピュータ読み取り可能な記録媒体である。

【００４６】このような記録媒体をコンピュータに組み込むことによって、暗号鍵を生成すると共にその暗号鍵をメモリ手段に格納する伝送用通信機器を構成することができる。

【００４７】

【発明の実施の形態】以下、本発明の好適な実施の形態を図面に基づいて説明する。

【００４８】実施の形態１

図１には、本実施の形態１のファイアーウォールモジュール（Fire Wall Module）１０の構成ブロック図が示されている。この図に示すように、ファイアーウォールモジュール１０は、インターネット等の外部ネットワーク１２と社内ネットワーク等の内部ネットワーク１４とを結ぶファイアーウォールモジュール１０である。また、ファイアーウォールモジュール１０は、この内部ネットワーク１４に接続するためのインターフェース１６ａを備えている。

【００４９】さらに、ファイアーウォールモジュール１０は、外部ネットワーク１２と接続するためのインターフェース１６ｂを有している。そして、ファイアーウォールモジュール１０は、外部ネットワーク１２と、内部ネットワーク１４との間のデータの流れを制御するシーケンサ１８を備えている。

【００５０】このシーケンサ１８は、アクセステーブルを有しており、このアクセステーブルの内容に従って、相手先によってはデータの暗号化や復号化を行う。

【００５１】ファイアーウォールモジュール１０は、本発明の伝送用通信機器の一例であり、シーケンサは、本発明の暗号化復号化手段の一例である。

【００５２】本実施の形態１において特徴的なことは、ファイアーウォールモジュール１０が、コンフィグレー

ションインターフェース２０を備えていることである。このコンフィグレーションインターフェース２０は、外部のリモートコントローラ３０とのデータ通信によって、暗号鍵とＩＤを自動生成する。そして、生成した暗号鍵とＩＤは、リモートコントローラ３０に送信されると共に、認証ブロック２１に送られる。さらに、暗号鍵とＩＤはリモートコントローラ３０にも送信される。データ通信は、種々の通信手法を採用することが好ましい。たとえば、赤外線通信や、電波による無線通信を行うことが好ましい。本発明の請求項における「無線」とは、この電波による無線通信を意味する。リモートコントローラ３０については後に詳述する。

【００５３】コンフィグレーションインターフェース２０は、本発明の暗号鍵管理手段の一例である。また、認証ブロック２１は、本発明における暗号鍵格納手段の一例である。

【００５４】また、上述したように、シーケンサ１８は、暗号化／復号化を実行するが、その際に利用する暗号鍵は、認証ブロック２１から必要に応じて供給される。

【００５５】本実施の形態１において特徴的なことは、ファイアーウォールモジュール１０が、認証ブロック２１を備えていることである。この認証ブロック２１は、ファイアーウォールモジュール１同士が通信を行う際に、相手側のファイアーウォールモジュールの識別動作を主に実行する。

【００５６】このような認証ブロック２１を備えることによって、ファイアーウォールモジュール１０同士による安全な通信を実現することができる。この認証ブロック２１の動作については後に詳述する。

【００５７】リモートコントローラ３０の構成ブロック図が図２に示されている。この図に示すように、リモートコントローラ３０は、コンフィグレーションインターフェース２０との通信手段３２と、制御手段３４と、メモリ手段３６と、を備えている。また、制御手段３４にはボタンスイッチ３４ａとボタンスイッチ３４ｂとが接続している。

【００５８】通信手段３２は、赤外線通信や無線通信によって、コンフィグレーションインターフェース２０との通信を行う手段である。制御手段３４はこの通信手段３２を用いてコンフィグレーションインターフェース２０との間で暗号鍵やＩＤの生成に必要なデータの送受信、さらにはコンフィグレーションインターフェース２０が生成した暗号鍵及びＩＤの受信、等を行う。

【００５９】制御手段３４は、利用者がボタンスイッチ３４ａを押下した場合、通信手段３２を介してコンフィグレーションインターフェース２０に新たな暗号鍵及びＩＤの生成を指示する。この指示に基づき、コンフィグレーションインターフェース２０は新たな暗号鍵及びＩＤを生成し、生成した暗号鍵とＩＤをリモートコントローラ３０に送信してくる。

【００６０】また、制御手段３４は、通信手段３２がコンフィグレーションインターフェース２０から生成した暗号鍵とＩＤとを受信した場合、この暗号鍵及びＩＤをメモリ手段３６に格納する。このメモリ手段３６は、リモートコントローラ３０から着脱自在に構成されており、リモートコントローラ３０以外のパーソナルコンピュータや各種通信装置に接続可能に構成されている。メモリ手段３６は、たとえば各種ＩＣカードや各種のフラッシュメモリを用いることが好ましい。もちろん、フレキシブルディスク等の磁気記録手段を利用してもかまわない。

【００６１】さらに、制御手段３４は、利用者がボタンスイッチ３４ｂを押下した場合、メモリ手段３６に格納されている暗号鍵及びＩＤを読み出し、通信手段３２を介してコンフィグレーションインターフェース２０にその暗号鍵及びＩＤを送信する。暗号鍵及びＩＤを送信されたコンフィグレーションインターフェース２０は、その暗号鍵及びＩＤを認証ブロック２１に送信する。認証ブロック２１はこの暗号鍵とＩＤとを内部に格納する。

【００６２】このような構成によって、利用者はこのメモリ手段３６を外部に持ち出し、他のファイアーウォールモジュール１０にこのメモリ手段３６を介して暗号鍵とＩＤとを供給することができる。又は、外部から受け取ったメモリ手段３６をリモートコントローラ３０に取り付け、このメモリ手段３６内に格納されている暗号鍵及びＩＤを、ファイアーウォールモジュール１０内に送ることができる。

【００６３】このようにして、複数のファイアーウォールモジュール１０に対して共通の暗号鍵とＩＤとを設定することができる。その結果、利用者は外部の他のファイアーウォールモジュール１０を用いて外部ネットワーク１２から内部ネットワーク１４にアクセスし、ＩＤと暗号鍵を用いた安全な通信を実行することが可能である。

【００６４】ここで、他のファイアーウォールモジュール１０は、他の場所にあるプライベートなネットワークとインターネットを結ぶ箇所に設けることができる。この場合は、そのプライベートなネットワーク上の電子機器から上記アクセスを行うことができる。

【００６５】また、他のファイアーウォールモジュール１０は、個別の電子機器の中に設けても良い。電子機器としては、たとえばパーソナルコンピュータや、携帯電話等を利用することができる。この場合は、利用者は、携帯電話等から、いわゆる移動体通信を利用して内部ネットワーク１４に対するアクセスを行うことができる。なお、電子機器としては、いわゆるＰＤＡ（Personal Digital Assistant）等の通信装置を利用してもかまわない。

【００６６】このファイアーウォールモジュール１０

は、本発明の「伝送用通信機器」の一例に相当する。

【００６７】また、このリモートコントローラ３０は、請求項の「制御機器」の一例である。

【００６８】次に、本実施の形態１における具体的な動作原理を図３、図４、図６、図７、図８のフローチャートを用いて詳細に説明する。

【００６９】まず、ステップＳ３－１においては、利用者が外部からアクセスするための暗号鍵とＩＤを生成するために、リモートコントローラ３０を利用して、コンフィグレーションインターフェース２０に対して、暗号鍵の生成を指示する。

【００７０】この指示においては、暗号鍵とＩＤの生成に必要なデータの送信が、リモートコントローラ３０からコンフィグレーションインターフェース２０に対して行われる。このデータには、利用者の名称や、乱数、日付・時刻のデータ、等を含めても良い。

【００７１】具体的な利用者の指示動作は、リモートコントローラ３０のボタンスイッチ３４ａの押下によって実行される。このボタンスイッチ３４ａの押下を制御手段３４が検知し、暗号鍵とＩＤの生成を通信手段３２を介してコンフィグレーションインターフェース２０に対して指示するのである。

【００７２】したがって、本実施の形態１によれば、利用者がファイアーウォールに関する知識を有していなくても、単にボタンスイッチ３４ａを押下するだけで暗号鍵とＩＤを生成させることができる。このファイアーウォール等に代表されるネットワーク機器の設定は非常に煩雑なものである。したがって、従来は、出張者が出張先から社内ネットワーク１４にアクセスするために新たに暗号鍵を生成しようと思っても、簡単に暗号鍵とＩＤを生成させることはできなかった。このような状況下でも本実施の形態１によれば、ネットワーク機器に詳しくない者でも暗号鍵とＩＤを容易に生成させることができるため、利便性の高いネットワークシステムを構築することができる。

【００７３】ステップＳ３－２においては、コンフィグレーションインターフェース２０が上記指示に基づいて暗号鍵とＩＤを生成する。この暗号鍵とＩＤは具体的にはそれぞれ8バイト程度のデータ列である。暗号鍵は、シーケンサ１８におけるデータの暗号化に利用されるデータである。また、ＩＤは利用者の「識別子」であり、通信している者を特定する役割を果たす。ただし、本実施の形態１では、このファイアーウォールモジュール１０を利用する者はすべて共通のＩＤを用いる例を説明している。したがって、本実施の形態１におけるＩＤはグループのＩＤ（識別子）とも言える。

【００７４】ステップＳ３－３においては、この暗号鍵とＩＤとが認証ブロック２１に送られる。この送信は暗号鍵とＩＤとを作成したコンフィグレーションインターフェース２０が実行する。認証ブロック２１は、送られてきた暗号鍵とＩＤとを内部に保存する。シーケンサ１８は、データの暗号化／復号化の際に、認証ブロック２１が格納している暗号鍵を利用する。

【００７５】ステップＳ３－４においては、この暗号鍵とＩＤがリモートコントローラ３０にも送られる。リモートコントローラ３０においては、通信手段３２を介して受信したこの暗号鍵とＩＤがメモリ手段３６に格納される。なお、ステップＳ３－３とステップＳ３－４の実行順序は逆でもかまわない。実際には、これらの送信はほとんど同時に実行されよう。この送信も、暗号鍵とＩＤとを作成したコンフィグレーションインターフェース２０が実行する。

【００７６】ステップＳ３－５においては、利用者はリモートコントローラ３０からメモリ手段３６を取り外し、内部ネットワーク１４に直接アクセスできない外部に持ち出す。このような状況は、たとえば他の支店や、出張等の状況が考えられる。そして、このメモリ手段３６を他の支店に設置されているファイアーウォールモジュール１０に付属するリモートコントローラ３０に取り付ける。出張等の場合は、このメモリ手段３６を出張者が携帯するノート型コンピュータに内蔵されているファイアーウォールモジュール１０に付属するリモートコントローラ３０に取り付ける。

【００７７】なお、リモートコントローラ３０は、内部ネットワーク１４側と、外部ネットワーク側１２との間で共用してもかまわない。すなわち、メモリ手段３６をリモートコントローラ３０から取り外さずに、リモートコントローラ３０ごと外部に持ち出し、支店のファイアーウォールモジュール１０と無線による通信を行わせても良い。また、リモートコントローラ３０ごと外部に持ち出し、ノート型パーソナルコンピュータ内部のファイアーウォールモジュール１０と通信を行わせても良い。

【００７８】さらに、ステップＳ３－５においては、利用者は、メモリ手段３６内に格納されている暗号鍵とＩＤとを他の支店等におけるファイアーウォールモジュール１０に供給する。この供給は、利用者がリモートコントローラ３０を操作することによって実行する。この実行によって、他の支店等に設けられているファイアーウォールモジュール１０中の認証ブロック２１中に、ＩＤと暗号鍵が格納される。

【００７９】具体的には、利用者はリモートコントローラのボタンスイッチ３４ｂを押下する。このボタンスイッチ３４ｂの押下を制御手段３４が検知し、メモリ手段３６内に格納されている暗号鍵とＩＤを通信手段３２を介してファイアーウォールモジュール１０内のコンフィグレーションインターフェース２０に送信するのである。コンフィグレーションインターフェース２０は、暗号鍵とＩＤとが送信されてくると、これらを認証ブロック２１に送る。認証ブロック２１は送られてきた暗号鍵とＩＤとを内部に格納する。

【００８０】このようにして複数のファイアーウォールモジュール１０に対して同一の暗号鍵とＩＤを設定することができる。これらのファイアーウォールモジュール１０同士の通信においてはこれらの暗号鍵とＩＤを用いた安全な通信を行うことができる。

【００８１】ステップＳ３－６においては、利用者が外部の支店や、出張先等からファイアーウォールモジュール１０を介して内部ネットワーク１４にアクセスを行う。このように、本動作例１においては、同一の暗号鍵及びＩＤが設定されたファイアーウォールモジュール１０同士がインターネット等の公衆ネットワークを介して通信を行う例を示す。

【００８２】ステップＳ３－６におけるファイアーウォールモジュールの詳細な動作を図４、図６、図７、図８のフローチャートに基づき説明する。

【００８３】図4は、ファイアーウォールモジュール１０を介して内部ネットワーク１４から外部ネットワーク１２に対してデータを送信する場合のファイアーウォールモジュール１０の動作を表すフローチャートである。

【００８４】また、図６、図７、図８は、外部ネットワーク１２から送られてきたデータをファイアーウォールモジュール１０を介して内部ネットワーク１４側が受信する場合のファイアーウォールモジュール１０の動作を表すフローチャートである。

【００８５】送信動作（図４）

まず、ステップＳ４－１において、シーケンサ１８は、内部ネットワーク１４からパケットを受信する。そして、シーケンサ１８は、このパケットの情報を検査し、そのＩＰヘッダー又はＴＣＰヘッダーの内容がアクセステーブルに登録されているか否かを検査する。前述したように、シーケンサ１８はその内部にアクセステーブルを有している。

【００８６】アクセステーブルの様子を表す概念図が図５に示されている。この図に示すように、アクセステーブルは、パケット情報と、ディスティネーションポートナンバー（Destination Port Number）と、暗号化ビットとを含むテーブルである。このテーブルへのデータのエントリー動作、及び暗号化ビットの制御動作については順次説明していく。

【００８７】さて、ステップＳ４－１における検査の結果、登録されている場合には、ステップＳ４－２に処理が移行し、登録されていない場合は、ステップＳ４－４に処理が移行する。

【００８８】ステップＳ４－２においては、その登録内容を検査し、暗号化ビットが立っているか否かを検査する。暗号化ビットが立っている場合には、ステップＳ４－３に処理が移行し、立っていない場合には、ステップＳ４－５に処理が移行する。

【００８９】ステップＳ４－３においては、暗号化鍵でパケットのデータペイロード部を暗号化する。暗号化した後、そのパケットをインターフェース１６ｂを介して外部ネットワーク１２に送り出す。

【００９０】この暗号化に際しては、シーケンサ１８は、認証ブロック２１から暗号化鍵を受け取り、暗号化に利用する。

【００９１】なお、本実施の形態１のファイアーウォールモジュール１０は、暗号化鍵を一度に一種類用いる。すなわち、ファイアーウォールモジュール１０を利用する人々は、すべて共通の暗号化鍵及びＩＤを利用するのである。暗号化鍵を更新する必要がある場合には、再びリモートコントローラ３０を操作して暗号化鍵及びＩＤの生成作業を実行する。そして、生成した暗号化鍵及びＩＤを各ファイアーウォールモジュール１０内の認証ブロック２１に格納するのである。

【００９２】もちろん、利用者のグループごとに別個の暗号化鍵及びＩＤを設けるように構成しても良い。

【００９３】ステップＳ４－４においては、そのパケットをアクセステーブルに新たに登録する。登録はそのパケットのパケット情報をテーブルに格納することによって実行する。

【００９４】パケット情報とは、ＩＰフィールドや、ＴＣＰ／ＵＤＰフィールドの情報を言い、たとえばＩＰヘッダーやＴＣＰヘッダー等の情報を意味する。少なくともパケット情報にはＩＰフィールド又はＴＣＰ／ＵＤＰフィールドの情報が含まれる。

【００９５】そして、ディスティネーションポートナンバーも格納する。さらに、テーブル中の各レコードには、暗号化ビットが設けられている。このように、アクセステーブルの各レコードは、パケット情報と、ディスティネーションポートナンバーと、暗号化ビットとから構成される。暗号化ビットの初期値は立っていない状態「０」である。

【００９６】ステップＳ４－５においては、パケットが暗号化されずにそのままインターフェース１６ｂを介して外部ネットワーク１２に送り出される。

【００９７】受信動作（図６、図７、図８）

まず、ステップＳ６－１において、シーケンサ１８は、外部ネットワーク１４からパケットを受信する。すると、シーケンサ２１は、認証ブロック２１内のアクセステーブルを読み出し、シーケンサ１８が受信したパケットのディスティネーションポートナンバーがアクセステーブルに格納されているか否か検査する。その結果、アクセステーブル中に一致するディスティネーションポートナンバーがあれば、ステップＳ６－２に処理が移行し、一致するものがなければ、ステップＳ６－５に処理が移行する。

【００９８】ステップＳ６－２においては、アクセステーブルとの比較が続行される。具体的には、他のパケット情報も一致するか否か検査される。この結果、一致すれば、ステップＳ６－３に処理が移行し、一致しない場

合にはステップＳ６－４に処理が移行する。

【００９９】ステップＳ６－３においては、そのパケットを内部ネットワーク１４に向けて送信する。すなわち、内部ネットワーク１２へ侵入するのを許可するのである。この際、アクセステーブルの暗号化ビットが立っている場合には、復号化処理を行ってもかまわない。このように暗号化・復号化処理を行うことによって、通信内容を第三者に知られてしまうことを防止することができる。

【０１００】ステップＳ６－４においては、外部から送信されてきたパケットを廃棄すると共に、そのパケットの送信元へ、応答パケットを送信する。この応答パケットの役割については後述する。

【０１０１】ステップＳ６－５においては、ディスティネーションポートナンバーがファイアーウォールモジュール１０用のポートナンバーであるか否か検査される。この検査の結果、一致すれば図７のステップＳ７－１に処理が移行し、不一致であればステップＳ６－６に処理が移行する。

【０１０２】さて、ファイアーウォールモジュール１０がパケットを生成した場合に、それに特化したポート番号がアサインされるが、そのポート番号を、ファイアーウォールモジュール１０用のポートナンバーと言う。

【０１０３】なお、一致したと言うことは、そのパケットはファイアーウォールモジュール１０宛のパケットであることを意味する。

【０１０４】ステップＳ６－６においては、外部から送られてきたパケットが廃棄される。ポート番号に該当するものがなく、エラーが発生していると考えられるからである。

【０１０５】図７のステップＳ７－１においては、パケットのデータペイロード部を認証ブロック２１に格納されている暗号鍵を用いて復号化する。

【０１０６】本実施の形態１においては、ファイアーウォールモジュール宛のパケットのデータペイロード部には、ＩＤを格納しておく取り決めを行っている。このような取り決めを行うことにより、不正なアクセスを防止することが可能である。

【０１０７】ステップＳ７－２では、復号化したＩＤを、既に登録済みのＩＤと比較する。比較の結果、一致すればステップＳ７－３に処理が移行し、一致しなければ図８のステップＳ８－１に処理が移行する。

【０１０８】ステップＳ７－３においては、アクセステーブルのチェックが実行される。具体的にはＩＰアドレスの一致等を検査するのである。

【０１０９】ステップＳ７－４においては、アクセステーブルのチェックの結果、パケットの送信者が既にアクセステーブルに登録されていればステップＳ７－５に処理が移行し、登録されていない場合には、ステップＳ７－９に処理が移行する。

【０１１０】ステップＳ７－５においては、ＩＤを所定量だけインクリメントする。この量もあらかじめ取り決めておく。このような量をあらかじめ取り決めておくことによって、インクリメント後のＩＤを受信した通信の相手側が当方を正しい通信相手と認識することが可能である。

【０１１１】ステップＳ７－６においては、インクリメント後のＩＤを暗号化する。暗号化は認証ブロック２１に格納されている暗号鍵を利用して実行する。

【０１１２】ステップＳ７－７においては、この暗号化したＩＤをデータペイロード部に含むパケットを、外部ネットワーク１２を介して、先にパケットを送信してきた送信元に送る。これはいわば送信元にアクノリッジを返したことになる。

【０１１３】ステップＳ７－８においては、アクセステーブル中の、上記送信元の暗号化ビットを立てて、「１」にする。これによって、以降、その送信元との間の通信は暗号化通信によって実行される。

【０１１４】ステップＳ７－９においては、外部から送られてきたパケットが廃棄される。

【０１１５】次に、ステップＳ８－１においては、受信したパケット中に格納されているＩＤを所定量だけデクリメントする。この量は上記インクリメントする量と同一である。

【０１１６】ステップＳ８－２においては、デクリメント後のＩＤが自己のＩＤと一致するか否か検査する。一致する場合には、ステップＳ８－３に処理が移行し、不一致の場合はステップＳ８－４に処理が移行する。

【０１１７】ステップＳ８－３においては、アクセステーブルにパケット情報を登録する。パケット情報とは、ＩＰフィールドや、ＴＣＰ／ＵＤＰフィールドの情報を言う。少なくとも、これらの情報には、ＩＰフィールド又はＴＣＰ／ＵＤＰフィールドの情報が含まれる。

【０１１８】ステップＳ８－４においては、パケット情報の登録に引き続き、その新たに登録したレコードの暗号化ビットを立てて「１」にする。これによって、以降、その送信元との間の通信は暗号化通信によって実行される。

【０１１９】ステップＳ８－５においては、ＩＤが一致しなかったのであるから、別グループのファイアーウォールモジュールからの通信が誤ってなされた等のエラーが発生している。したがって、そのパケットは廃棄される。

【０１２０】応答パケット

次に、応答パケットについて説明する。ファイアーウォールモジュール１０は、内部ネットワーク１４から送信されてきたパケットのみを外部ネットワーク１２に送信するだけでなく、自己が自ら構成したパケットを外部ネットワーク１２に送信することもある。これが上記ステップＳ６－４で言及した応答パケットである。

【0121】応答パケットの説明図が図9に示されている。

【0122】図9（1）には応答パケットが示されている。ここに示すように、応答パケットは、IPヘッダーと、TCPヘッダーと、IDが暗号化されたデータと、の3種類のブロックを含んでいる。ここで、TCPヘッダーにおいては、ディスティネーションポートナンバーは、ファイアーウォールモジュール10用のポートナンバーである。このファイアーウォールモジュール10用のポートナンバーを用いることによって、ファイアーウォールモジュール10に対するパケットであることを表すことができる。

【0123】なお、この応答パケットは、認証ブロック21が作成する。認証ブロック21は、外部からパケットが送信されてきた場合にこのような応答パケットを生成し、外部に出力する（上記ステップS6-4）。

【0124】図9（2）には、応答パケットを受信したファイアーウォールモジュール10がその応答パケットを受領した旨を表す承認パケットの説明図が示されている。この承認パケットは、上記ステップS7-7において送信されるパケットである。この図に示すように、承認パケットは、IPヘッダーと、TCPヘッダーと、所定量インクリメントされたIDが暗号化されたデータと、の3種類のブロックを含んでいる。ここで、TCPヘッダーにおいては、ソースポートナンバーは、ファイアーウォールモジュール10用のポートナンバーである。このファイアーウォールモジュール10用のポートナンバーを用いることによって、ファイアーウォールモジュール10が送信したパケットであることを表すことができる。

【0125】なお、この承認パケットも、認証ブロック21が作成する。認証ブロック21は、応答パケットを受信した場合にこの承認パケットを送信することによって暗号通信の準備が完了したことを相手側に伝えることができる。

【0126】以上述べたような動作を本ファイアーウォールモジュール10は実行する。このような動作によって、具体的には以下のような通信モードを実現することができる。

【0127】通信モード1（ファイアーウォールモジュール同士の通信）

ファイアーウォールモジュール10同士の通信においては、既に述べたように、あらかじめリモートコントローラ30やメモリ手段36によって、共通の暗号鍵及びIDが各ファイアーウォールモジュール10に設定されている。

【0128】通信モード1の動作を説明するシーケンス図が図10に示されている。

【0129】まず、一方のファイアーウォールモジュール10aを含む通信システムから、他方のファイアーウォールモジュール10bを含む通信システムへパケットが送信される（100）。この送信の際、新しい相手先であればアクセステーブルに登録されることは既に説明した通りである（ステップS4-4）。

【0130】次に、上述したように、ステップS6-6に従って、他方のファイアーウォールモジュール10bの認証ブロック21は応答パケットを生成し、これを一方のシステムに返送する。これが図中102で示されている。この応答パケットは暗号化されたIDを含んでいる。

【0131】応答パケットを受信した一方のファイアーウォールモジュール10aは、IDを復号し（ステップS7-1）、アクセステーブルに登録してあるのを確認し（ステップS7-4）、ステップS7-7において承認パケットを他方のファイアーウォールモジュール10に返送する。これは図中104で示されている。さらに、暗号化ビットも立てられる（ステップS7-8）。

【0132】承認パケットを受信した他方のファイアーウォールモジュール10bは、ステップS8-1でIDをデクリメントした結果元のIDが得られることを確認した後（ステップS8-2）、アクセステーブルにパケット情報を登録し、暗号化ビットを立てる。

【0133】以上のようにして、両システムがそれぞれアクセステーブルに登録され、パケットは、ファイアーウォールモジュール10を通過する際に自動的に暗号化、復号化される。そのため、暗号通信を容易に実行することができる。

【0134】通信モード2（ファイアーウォールモジュール10を用いない相手先）

ファイアーウォールモジュール10は、そのシーケンサ18中にアクセステーブルを有しているため、通信相手がファイアーウォールモジュール10を有しない場合でも、通常通りの通信を実行することが可能である。

【0135】既に述べたように、ファイアーウォールモジュール10を用いて外部にパケットを送信する場合には、新しい相手であれば必ずアクセステーブルに登録がなされる（ステップS4-4）。

【0136】したがって、一度アクセスした相手先からパケットが送られてきた場合には、必ずアクセステーブル内のパケット情報と合致するはずである（ステップS6-2、S6-3）。したがって、暗号化の対象とはならず、従来の通常の通信を行うことが可能である。

【0137】以上述べたように、本実施の形態1によれば、ファイアーウォールモジュール10を用いることによって、たとえば家庭内ネットワークに、外部から公衆ネットを介して安全にアクセスすることが可能である。特に、アクセスする権利を有する利用者群に共通のIDを設定しているため、そのIDを用いたアクセス以外を拒否することができ、安全に通信を行うことが可能である。IDが異なることによって、たとえば「他の家庭の

家庭内ネットワーク」に対するアクセスであると判断することができるものである。

【0138】本実施の形態1によれば、内部ネットワーク14に外部ネットワーク12からアクセスするための暗号鍵とIDを自動的に作成し、さらにその暗号鍵とIDがメモリ手段36に格納されるため、そのメモリ手段36を用いて外部ネットワーク12から容易に保護ネット14へアクセスすることが可能となる。

【0139】そして、第三者の内部ネットワーク14への侵入を防止しつつ、内部ネットワーク14へアクセスする正当な権利を持つ者は、外部ネットワーク12から容易に内部ネットワーク14にアクセスすることができる。

【0140】なお、コンフィグレーションインターフェース20は、赤外線通信や無線通信を行う通信装置と、暗号鍵を生成するプログラムとそのプログラムを実行するプロセッサとから構成される。このプログラムは、図3に示す動作の一部を実行し、リモートコントローラ30からの指示によって暗号鍵とIDを生成し、シーケンサ18や、認証ブロック21、リモートコントローラ30に送信する。

【0141】また、コンフィグレーションインターフェース20と、リモートコントローラ30との間の通信はIrDA等の赤外線通信、Blue Tooth等の無線通信、等を利用することができる。なお、IrDAとは、業界内の標準化組織であるInfrared Data Associationが赤外線データ通信の規格として標準化を行った規格である。Blue Toothとは、複数の電気通信会社が制定した無線通信の規格の名称であり、商標でもある。

【0142】また、リモートコントローラ30の制御手段34は、プログラムとそのプログラムを実行するプロセッサとから構成されている。

【0143】このファイアーウォールモジュール10は、本発明の「伝送用通信機器」の一例に相当する。

【0144】このリモートコントローラ30は、請求項の「制御機器」の一例である。

【0145】ファイアーウォールモジュールの構成
ファイアーウォールモジュール10は、実際にはLSIで構成することが好ましい。特にシーケンサ18は高速性が要求される場合が多いと考えられるため、ハードウェアで実現することが望ましい場合が多い。

【0146】しかし、高速性がそれほど要求されない用途では、ファイアーウォールモジュール10はプログラムと、そのプログラムを実行するプロセッサとから構成しても良い。このプログラムは、これまで述べたフローチャートに示された動作をコンピュータに実行させるプログラムである。これらのプログラムをハードディスク等の記憶手段に格納したコンピュータを用いて上記ファイアーウォールモジュールと同様の機能を実現することができる。このような構成を表す説明図が図11に示されている。

【0147】この図に示すように、コンピュータ120は、内部のハードディスク122にこれまで述べた動作を実現するプログラムを格納している。そして、プロセッサ124がこのプログラムを実行する。内部ネットワーク14とのインターフェース16aや、外部ネットワークとのインターフェース16bそのものはIEEE802.3等のインターフェースであり、ハードウェアで実現することが好ましい。ただし、外部のリモートコントローラ30とのインターフェースはたとえばIrDA等のインターフェース200を利用することが好ましいが、他のブルートゥース（Blue Tooth）等のインターフェースを利用してもかまわない。また、プログラムはハードディスク122に限らず、種々の光ディスク、半導体記憶装置等を利用しても良い。

【0148】なお、インターフェース16a、16bはハードウェアで実現するのが好ましいと述べたが、そのインターフェースの制御部分はプログラムで構成することが好適であろう。コンフィグレーションインターフェース20の無線通信の部分は、上述したようにIrDAやBloo Toothのインターフェースであるが、このインターフェース部分に関してもそのハードウェアの制御はプログラムによって実現することが好ましい。これらのプログラムもハードディスク122に格納しておく。また、図1における認証ブロックは、暗号鍵を保管するが、その保管場所はハードディスク102を利用することが好ましい。すなわち、図11の構成の場合は、図1における認証ブロックは、ハードディスク122内のプログラムだけでなく、その内部の記憶領域によって実現されている。また、図1におけるシーケンサ内部のアクセステーブルも同様にハードディスク122内の記憶領域を用いて構成することが好適である。

【0149】実施の形態2
上記実施の形態1では、リモートコントローラ30にメモリ手段36を装着し、リモートコントローラ30を介して暗号鍵やIDをメモリ手段36に格納した。

【0150】しかし、コンフィグレーションインターフェース20から直接メモリ手段36に暗号鍵やIDを書き込んでも良い。また、コンフィグレーションインターフェース20が、メモリ手段36に格納された暗号鍵やIDを直接読みとっても良い。

【0151】このような構成を表す図が図12に示されている。この図に示すように、コンフィグレーションインターフェース20には、メモリインターフェース22が接続されている。このメモリインターフェース22は、メモリ手段36がICカードの場合には、ICカードリーダ／ライタである。また、メモリ手段36がフラッシュメモリの場合には、フラッシュメモリのリーダ／ライタを用いる。要するに、メモリ手段36にデータを読み書きできる手段であればどのようなものでも良い。

【0152】また、近年ＵＳＢインターフェースプラグの中にフラッシュメモリ等を組み込んだメモリ製品が利用されている。このようなＵＳＢプラグを利用したメモリをメモリ手段３６として用いる場合は、メモリインターフェース２２として、ＵＳＢインターフェースを使用することができる。このように構成すれば、メモリ以外に他のＵＳＢインターフェースを有する機器もファイアーウォールモジュール１０に接続することができ、汎用性が高まる。

【0153】なお、図１２のような構成を採用した場合、利用者は、リモートコントローラ３０のボタンを押下する代わりにファイアーウォールモジュール１０に接続されているボタンスイッチ２４ａを押下することによって、暗号鍵及びＩＤの生成を指示する。この場合、コンフィグレーションインターフェース２０のプログラムは、ボタンスイッチ２４ａが押下された場合に暗号鍵及びＩＤの生成を開始するような動作を実行する。

【0154】さらに、コンフィグレーションインターフェース２０は、生成した暗号鍵及びＩＤを、認証ブロック２１に送信し、メモリ手段３６に書き込む。書き込みは、メモリインターフェース２２を用いて実行される。

【0155】逆に、メモリ手段３６に格納された暗号鍵及びＩＤを読み取り、認証ブロック２１に格納する動作を実行させるには、利用者はボタンスイッチ２４ｂを押下する。利用者がボタン２４ｂを押下すると、コンフィグレーションインターフェース２０のプログラムは、この押下に応じて、メモリ手段３６から暗号鍵及びＩＤを読み出し、認証ブロック２１に送信する。認証ブロック２１はこの暗号鍵とＩＤとを内部に格納する。なお、メモリ手段３６からの読み出しは、メモリインターフェース２２を用いて実行される。

【0156】このように本実施の形態１に示された構成を採用した場合でも、これを図１１に示されたようなプログラムを用いた構成としても良い。

【0157】

【発明の効果】以上述べたように、本発明によれば、暗号鍵を伝送用通信機器に自動的に生成させることが可能である。さらに、その暗号鍵を外部に取り出すことができるので、他の伝送用通信機器へ同一の暗号鍵を容易に導入させることが可能である。

【0158】また、本発明によれば、無線通信や赤外線通信によって伝送用通信機器に暗号鍵を自動的に生成させることができる。さらに、その暗号鍵を無線通信や赤外線通信を介して受信し、メモリ手段に格納することができる。その結果、メモリ手段を他のシステムに組み込み、他の伝送用通信機器に対して容易に同一の暗号鍵を導入することができる。

【0159】また、本発明によれば、外部からの暗号鍵を容易に伝送用通信機器に導入させることができる。

【図面の簡単な説明】

【図１】本実施の形態のファイアーウォールモジュールの構成ブロック図である。

【図２】リモートコントローラの構成ブロック図である。

【図３】本実施の形態１の動作を説明するフローチャートである。

【図４】本実施の形態１の動作を説明するフローチャートである。

【図５】アクセステーブルの構成を示す説明図である。

【図６】本実施の形態１の動作を説明するフローチャートである。

【図７】本実施の形態１の動作を説明するフローチャートである。

【図８】本実施の形態１の動作を説明するフローチャートである。

【図９】応答パケットと承認パケットの構成を示す説明図である。

【図１０】ファイアーウォールモジュール同士の通信を説明するシーケンス図である。

【図１１】コンピュータをファイアーウォールモジュールとして動作させるためのプログラムを用いた場合の構成図である。

【図１２】実施の形態２において、無線通信を使用しない場合のファイアーウォールモジュールの構成ブロック図である。

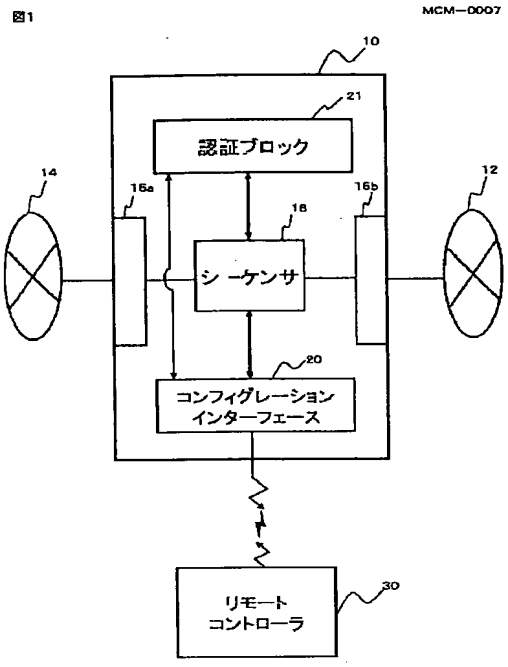
【符号の説明】

１０　ファイアーウォールモジュール
１０ａ　一方のファイアーウォールモジュール
１０ｂ　他方のファイアーウォールモジュール
１２　外部ネットワーク
１４　内部ネットワーク
１６ａ　インターフェース
１６ｂ　インターフェース
１８　シーケンサ
２０　コンフィグレーションインターフェース
２１　認証ブロック
２２　メモリインターフェース
２４ａ　ボタンスイッチ
２４ｂ　ボタンスイッチ
３０　リモートコントローラ
３２　通信手段
３４　制御手段
３４ａ　ボタンスイッチ
３４ｂ　ボタンスイッチ
３６　メモリ手段
１００　パケット送信
１０２　応答パケット
１０４　承認パケット
１２０　コンピュータ
１２２　ハードディスク

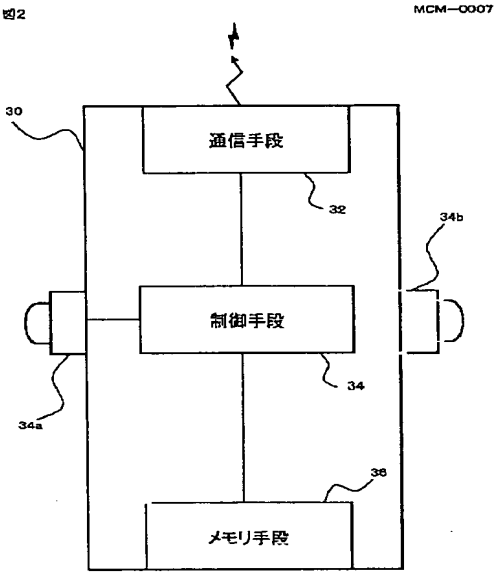
124　プロセッサ

200　インターフェース

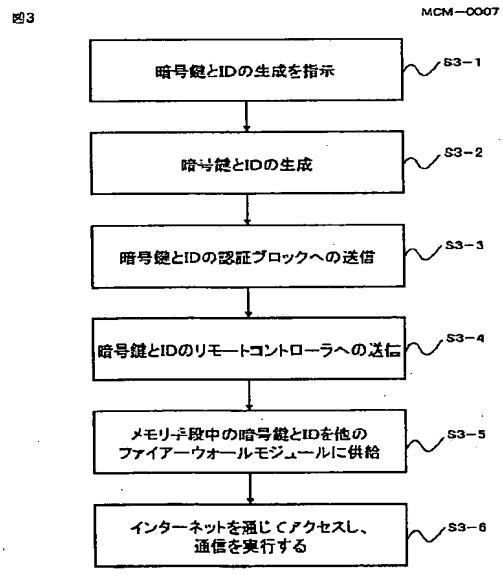
【図1】



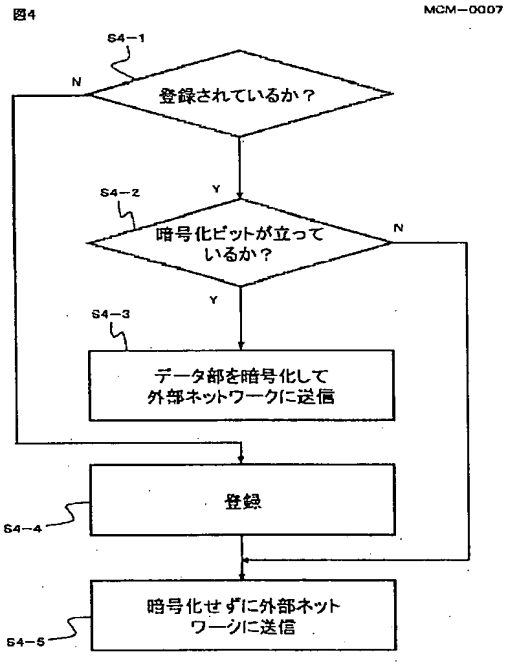
【図2】



【図3】



【図4】

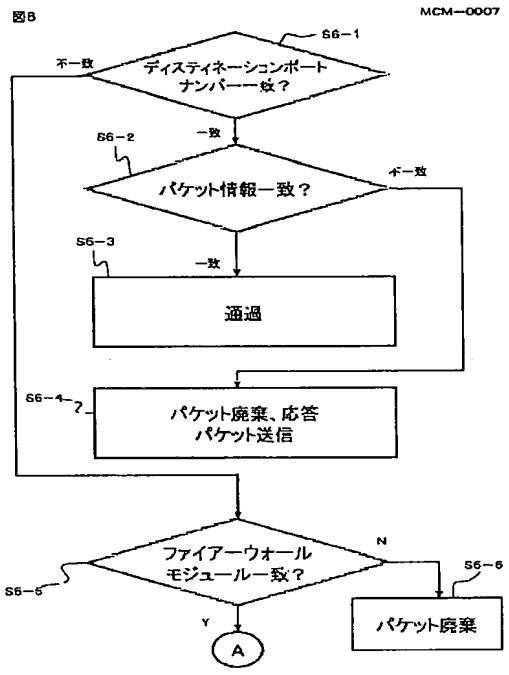


【図5】

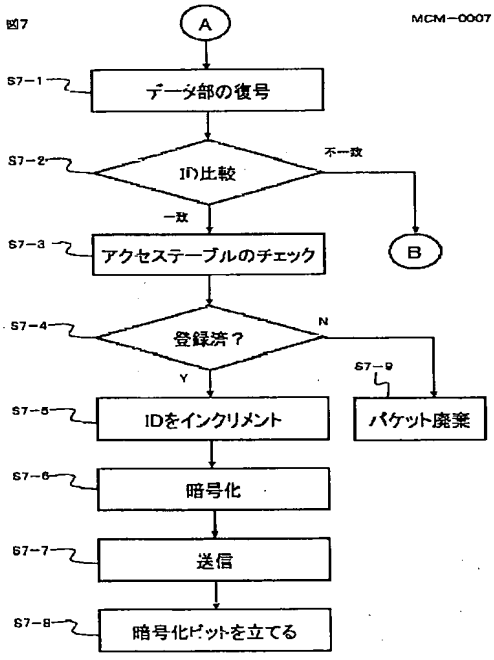
図5 MCM-0007

パケット情報	ディスティネーションポートナンバー	暗号化ビット
192. 168. 5. 0		0
193. 180. 7. 5		0
201. 200. 1. 128		1

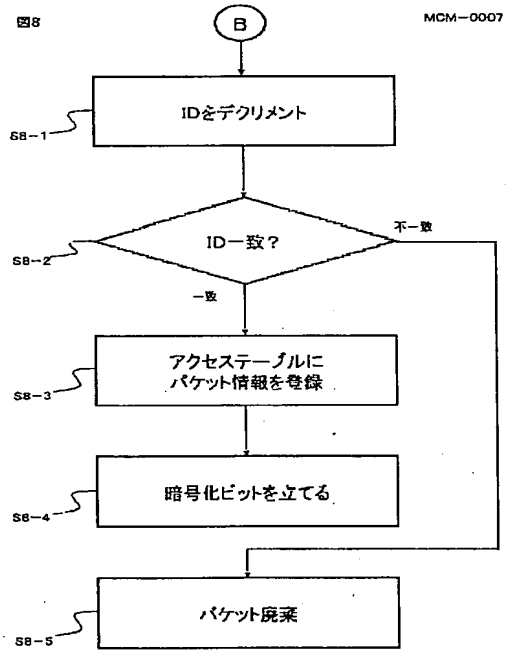
【図6】



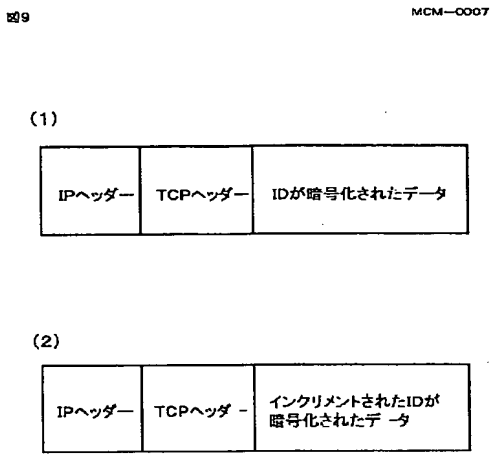
【図7】



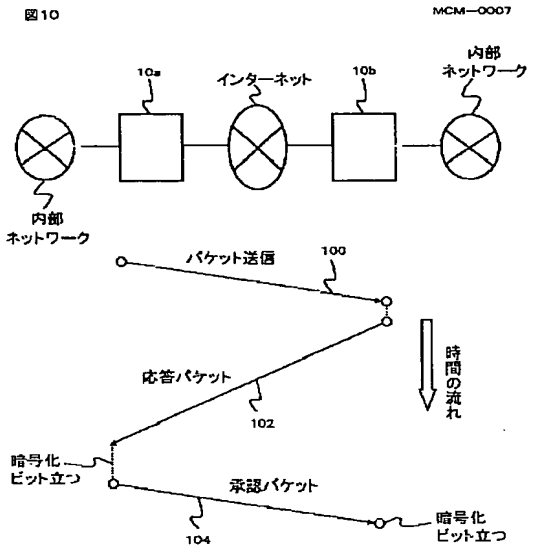
【図8】



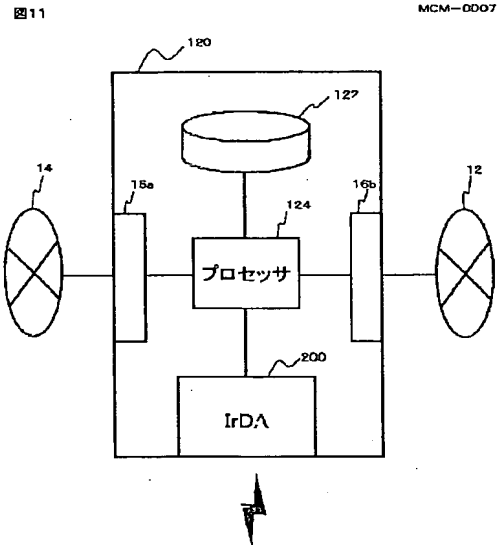
【図9】



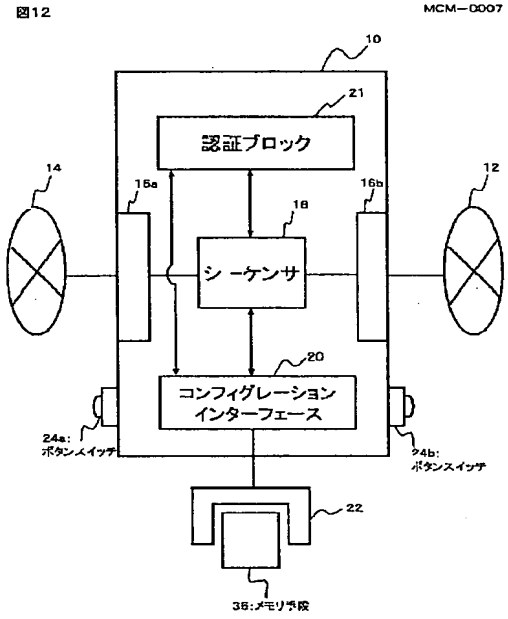
【図10】



【図11】



【図12】



フロントページの続き

Fターム(参考) 5B089 GA31 GB02 JB14 KA17 KB13
5J104 AA16 EA04 EA22 NA02 NA41
5K030 GA05 GA15 HA08 HC01 HC13
HD03 HD06 JL01 KA04 LD19